REPORT OF THE BUSINESS CONTINUITY COMMITTEE
TO THE HOMELAND SECURITY COUNCIL – JUNE 2003

TABLE OF CONTENTS

TABLE OF CONTENTS

(This page intentionally left blank.)

REPORT OF THE BUSINESS CONTINUITY COMMITTEE TO THE HOMELAND SECURITY COUNCIL – JUNE 2003

EXECUTIVE SUMMARY

SUBJECT:

Recommendations to Improve Business Continuity for Missouri State Government

OBJECTIVE:

Provide an overview and recommendations concerning issues that provide both near-term and long-term sustainable improvement to Business Continuity in Missouri. Obtain Homeland Security Council support for recommendations in the form of policies, procedures, Executive Orders and budget items consistent with improving Missouri's continuity capabilities. Business continuity relates specifically and significantly to state agencies' ability to continue to conduct business in catastrophic conditions or severe infrastructure failures.

BACKGROUND:

Business continuity, while it has the potential to have information technology implications, is purely a business operation issue. Disaster recovery as a related issue is an information technology issue and specifically relates to ensure the ability to recover critical information technology infrastructure during catastrophic events.

The Federal Office of Homeland Security has devoted significant resources to defining strategies to the continuity of government. Recent state audits have revealed consistent and troublesome deficiencies in the continuity capabilities of several state agencies, recognizing that no state department or agency has met the minimum standards. The state of Missouri must both develop and implement strategies and operational capabilities to continue to conduct business in catastrophic conditions or severe infrastructure failures.

VISION:

Ensure the existence of business continuity plans for each agency and disaster recovery plans for required critical information technology infrastructure assets so as to facilitate continued state agency business operations in a time of catastrophic events.

Missouri's initial vision must be focused upon the following goals and objectives:

A. Raise the awareness of and recognition of the need for business continuity plans and disaster recovery plans.

B. Clearly delineate the difference between state government operation plans and state agency business continuity plans and the corresponding responsibilities.

C. Develop a methodology for agencies to utilize in the development of business continuity plans.

D. Identify those information technology infrastructure assets that should be included in Missouri's Critical Asset Protection Plan and ensure that those assets are covered by an adequate disaster recovery plan.

EXECUTIVE SUMMARY

E. Recommend policies and procedures for the development, maintenance and annual exercising of business continuity and disaster recovery plans.

F. Develop a business plan that clearly articulates the issues surrounding economic impact of having and maintaining business continuity and disaster recovery.

RECOMMENDATIONS:

Executive Order to establish governance with the Office of Information Technology.

Legislative approval and appropriation of funds to support the OIT Business Continuity budget proposal.

Executive Order for Business Continuity
03-XX

WHEREAS, on September 11, 2002, I issued Executive Order 02-15 establishing the Missouri Security Council for the express purposes of coordinating homeland security-related activities between executive agencies and local political subdivisions and effective development and implementation of homeland security policies; and

WHEREAS, the Director of Homeland Security, was charged with determining the agenda of Missouri Security Council meetings, ensuring necessary papers are prepared, recording Council actions and recommendations, serving as the principal liaison to any federal Homeland Security offices or agencies and advising the Governor on all state Homeland Security issues; and

WHEREAS, the Director of Homeland Security, in meeting his charge, did establish a Business Continuity Committee for the express purpose of studying and making recommendations to ensure business continuity with respect to Missouri's critical business processes; and

WHEREAS, to ensure the existence of business continuity plans for each agency and disaster recovery plans for required business processes and critical assets so as to facilitate continued state agency business operations in a time of catastrophic events; and

WHEREAS, the state of Missouri must both develop and implement strategies and operational capabilities to continue to conduct business in catastrophic conditions or severe infrastructure failures, and

WHEREAS, to provide both near-term and long-term sustainable improvement to Business Continuity in Missouri;

NOW, THEREFORE, I, BOB HOLDEN, GOVERNOR OF THE STATE OF MISSOURI, by virtue of the authority vested in me by the constitution and the laws of the state of Missouri, do hereby order the following:

Section 1. Policy. It shall be the policy of the state of Missouri that each state department or agency shall work diligently to protect the critical assets and ensure the continuity of services of the State.

a) Each agency shall adopt policy consistent with the guidelines and model policy developed by the Business Continuity Committee of the Missouri Security Council and establish appropriate procedures to ensure the existence of business continuity plans for each agency to include disaster recovery plans for required critical information technology infrastructure assets so as to facilitate continued state agency business operations in a time of catastrophic events.

b) Each agency shall specifically address the issue of Business Continuity with any entity with whom it conducts critical business processes to determine if they have appropriate continuity controls in place.

Section 2. Office of Information Technology. The Office of Information Technology (OIT), in its role as chair of the Business Continuity Committee of the Missouri Security Council shall provide advice and make recommendations to the Homeland Security Council. OIT is responsible to coordinate Information Technology resources required to ensure uninterrupted access to essential capabilities in the event of a disaster and to provide technology guidance in Business Continuity Plans with the State Emergency Management Agency (SEMA). Such recommendations shall include:

a) Raise the awareness of and recognition of the need for business continuity plans and disaster recovery plans.

b) Clearly delineate the difference between state government operation plans and state agency business continuity plans and the corresponding responsibilities.

c) Develop a methodology for agencies to utilize in the development of business continuity plans.

d) Identify those information technology infrastructure assets that should be included in Missouri's Critical Asset Protection Plan and ensure that those assets are covered by an adequate disaster recovery plan.

e) Recommend policies and procedures for the development, maintenance and annual exercising of business continuity and disaster recovery plans.

f) Develop a business plan that clearly articulates the issues surrounding economic impact of having and maintaining business continuity and disaster recovery.

Section 3. Chief Information Officer. The Chief Information Officer (CIO) shall issue policies consistent with recommendations put forth by the Business Continuity Committee of the Missouri Security Council. The objective is to ensure that critical capabilities are provided without interruption, and restoration of other services is planned in sufficient detail to ensure success.

Section 4. Alteration of Authority. This order shall not be construed to alter the existing authorities of any executive agency or department, except that all executive departments and agencies are directed to assist the Chief Information Officer in carrying out the purposes of this order.

IN WITNESS WHEREOF, I have hereunto set my hand and caused to be affixed the Great Seal of the State of Missouri, in the City of Jefferson, on this xxth day of June, 2003.

[Bob Holden's signature]
BOB HOLDEN
GOVERNOR

ATTEST:

[Matt Blunt's signature]
SECRETARY OF STATE

ISSUE 1: RECOGNITION AND ESTABLISHMENT OF BUSINESS CONTINUITY PLANS

♦ **Business Continuity Management**

ISSUE DESCRIPTION:

Business Continuity Management (BCM) is not just about reacting to an incident. It's not just about disaster recovery, crisis management, risk management control or technology recovery. And it's not just a professional specialist discipline. BCM is a business owned and driven activity that can provide the strategic and operational framework to review the way Missouri State Government provides its products and services and increase its resilience to disruption, interruption or loss.

> ***Business Continuity Management is a holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response which safeguards the interests of its key stakeholders, citizens, and business entities.***

Business Continuity Management has also long been recognized as good business practice and is an integral part of corporate governance. Within this setting BCM takes on a strategic dimension and should not only be seen in a narrow reactive operational context. Enlightened organizations have already adopted this approach. Governments are also becoming keen to see effective BCM deployed at strategic levels in all government departments and agencies. Today good Business Continuity Management fully recognizes that an organization's resilience depends equally on its management and operational staff as well as technology and requires a holistic approach to be taken when establishing a BCM capability.

AUTHORIZATION:

September 11, 2002, Executive Order 02-15 establishing the Missouri Security Council which subsequently established a Business Continuity Committee for the express purpose of studying and making recommendations to ensure business continuity with respect to Missouri's critical information technology infrastructure.

ACTION REQUIRED:

Executive Order issued to establish governance within the Office of Information Technology.

Legislative approval and appropriation of funds to support the OIT Business Continuity budget proposal.

ISSUE 1: RECOGNITION AND ESTABLISHMENT OF BUSINESS CONTINUITY PLANS

♦ Business Continuity Management:

Missouri State Government must establish Business Continuity Plans (BCP), including obtaining management support and organizing and managing the project to completion within agreed upon time and budget limits, with the appropriate resources. Activities to be considered during the initiation process depend on the extent to which Business Continuity Management disciplines have been applied within the organization. Some parts of the business may have established individual continuity plans based around manual workarounds, whereas IT may have developed contingency plans for systems perceived to be critical. These should be identified and validated in the subsequent stages. As part of the project initiation it is essential to scope the initiatives. Careful consideration should also be given to the inclusion of critical third parties.

The Office of Administration, Office of Information Technology FY04 decision item "Continuous Availability Request" for Business Continuity states:

> Catastrophic events could shut down government services if business continuity plans are not addressed. Disasters that impact either the State Data Center or the telecommunications infrastructure would halt the delivery of services to law enforcement, social program recipients, state employees and virtually every citizen and business that conducts business with the state.

BUSINESS CASE:

Business Continuity Management (BCM) relates specifically and significantly to state agencies' ability to continue to conduct business in catastrophic conditions or severe infrastructure failures to ensure the maximum availability of essential services. Business Continuity Management is a business issue, with real benefits for any organization and must be considered an organization wide discipline with support from top management.

The Missouri Security Panel report (February 2002) recommended assessment of all critical infrastructure, including information systems. The *National Strategy for The Physical Protection of Critical Infrastructures and Key Assets* (February 2003); states "America's critical infrastructure sectors provide the foundation for our national security, governance, economic vitality, and way of life. Furthermore, their continued reliability, robustness, and resiliency create a sense of confidence and form an important part of our national identity and purpose." The National Governors Association publication, *A Governor's Guide to Emergency Management, Volume Two: Homeland Security* (September 2002); "addresses the major homeland security issues a governor and his or her staff need to understand and prepare for,…and outlines the interaction needed among the governor's office, the homeland security director, the state emergency management office, other state agencies, local governments, the private sector, volunteer organizations, and the federal government."

The Office of Administration, Office of Information Technology FY04 decision item "Continuous Availability Request" for Business Continuity states:

> This decision item is to assess the states ability to continue to conduct business in catastrophic conditions or severe infrastructure failures. As a result of the assessment a plan will be developed to provide continued State Data Center operations and the

operation of various state agencies to support business operations. Initially a study will be conducted to develop a deficiency report indicating the impact of failure. Subsequently, a plan would be developed to bring the state to 100% preparedness. The plan would include statewide infrastructure plans and agency plans. Additionally:

- A deficiency report would be developed to identify areas of impact
- A plan would be developed to bring the state into 100% preparedness to address data center and telecommunications infrastructure issues
- Local agency plans would be developed to provide for continuous service availability
- Contracts would be established and Data Center and telecommunications hot sights would be implemented
- Annual reviews of operational recovery plans would be done to ensure vitality for the recovery plan.
- Disaster drills would be executed for hot site testing. Paper drills would also be performed to ensure agency readiness.
- Plans will emphasis business recovery as well as technical infrastructure.

BENEFITS:

Realistic and relevant BCP planning results in improved, continuous delivery of government services to the public. The Office of Administration, Office of Information Technology FY04 decision item “Continuous Availability Request” for Business Continuity states:

Positive Results

- The State of Missouri would be in a position to provide continuous availability of services in the event of natural disaster.
- Public safety would be enhanced

Negative Results

- Confidence in governmental services would be reduced
- Lack of continuous availability of state services would impact the state and local economies

Objective #1: Provide computerized access to public information held by Missouri State Government.

- Appropriate Data Center Hot Site Available
- Agency Business Continuity Plans Available

Governmental services and public information are electronically available to Missouri citizens.

- In the event of a disaster, state technology services are recoverable within 120 hours
- In the event of a disaster state business operations are recoverable within 120 hours

ISSUE 1: RECOGNITION AND ESTABLISHMENT OF BUSINESS CONTINUITY PLANS

COST FACTORS:

The Office of Administration, Office of Information Technology FY04 decision item "Continuous Availability Request" for Business Continuity states:

> In FY03 the Office of Information Technology (OIT) received federal spending authority of $600,000 to perform an initial assessment of the states ability to provide continuous business availability would be conducted. This would include an inventory of all locations that would require a hot site, a determination of the current agency business continuity capabilities and a plan to address all deficiencies. The OIT is currently seeking these funds through the Homeland Security initiative.
>
> The second year of funding (FY04) would support continuous availability for the sites that are determined to be critical access sites. These sites are being determined by the Missouri Critical Assets Assessment Plan. FY04 funding would provide an annual review of operations capabilities as well as hot site facilities. *The FY04 request is for spending authority of $1,800,000 to be funded through the Homeland Security initiative for Professional Services.*
>
> The third year of funding would include an annual review of operations capabilities and hot sites to support all remaining agencies. *The proposed FY05 request is for spending authority of $2,700,000 to be funded through the Homeland Security initiative for Professional Services.*
>
> Funding would be required in all out years for annual review of operations capabilities as well as hot site reservation and testing costs.
>
> Funding costs are based on pricing submitted from respondents to an RFP conducted in early 2000. RFP content was based upon business requirements submitted by State Data Center (SDC) customers. Cost estimates have been increased slightly to allow for inflation and expansion of the program to cover all departments regardless of SDC customer status.

ISSUE 2: STATEWIDE METHODOLOGY FOR BUSINESS CONTINUITY PLANNING

- **Awareness and Training**
- **Risk Assessment**
- **Business Impact Assessment**
- **Business Continuity Strategies**
- **Business Continuity Plans**
- **Testing and Exercising Business Continuity Plans**

ISSUE DESCRIPTION:

Careful planning is essential in deciding how to best spend business continuity dollars. To achieve the state's best return on investment it must develop a statewide methodology for Business Continuity Planning. This methodology must include, but not be limited to:

A. Preparing a program to create government awareness and enhance the skills required to develop, implement, maintain, and execute the Business Continuity Plan.

B. Determining the events and environmental surroundings that can adversely affect the organization and its facilities with disruption as well as disaster, the damage such events can cause, and the controls needed to prevent or minimize the effects of potential loss. Providing cost-benefit analysis to justify investment in controls to mitigate risks.

C. Identifying the impacts resulting from disruptions and disaster scenarios that can affect the organization and techniques that can be used to quantify and qualify such impacts. Establishing critical functions, their recovery priorities, and inter-dependencies so that recovery time objective can be set.

D. Determining and guiding the selection of alternative business recovery operating strategies for recovery of business and information technologies within the recovery time objective, while maintaining the organization's critical functions.

E. Designing, developing, and implementing the Business Continuity Plan that provides recovery within the recovery time objective.

F. Pre-planning and coordinating plan exercises, and evaluating and documenting plan exercise results. Developing processes to maintain the currency of continuity capabilities and the plan document in accordance with the organization's strategic direction. Verifying that the Plan will prove effective by comparison with a suitable standard, and report results in a clear and concise manner.

AUTHORIZATION:

03-XX, Executive Order for Business Continuity, establishing policies and procedures for the purpose of conducting Business Continuity Planning for the State of Missouri.

ACTION REQUIRED:

Develop a committee to represent key stakeholders in developing, planning, and recommending the tools, templates, and processes necessary to develop Business Continuity standard methodologies. The committee will represent a diverse cross section of state agencies and business entities to ensure consistent practices and principles in developing plans.

ISSUE 2: STATEWIDE METHODOLOGY FOR BUSINESS CONTINUITY PLANNING

♦ Awareness and Training

Missouri State Government must prepare a program to create State Government awareness and enhance the skills required to develop, implement, maintain, and execute the Business Continuity Plan.

Organizations face numerous external and internal risks that can threaten the continuity of their business operations. Terrorism and cyber-vandalism have now been added to the traditional list of natural and man-made disasters such as fires, floods and power outages. Enterprises now have to ask themselves more and more hard questions: What if we can't get into our building? How fast can we get back up and running if our data center becomes inoperable? How do we prepare for the emergency that we can't even predict? Indeed many organizations are unsure of how to prepare and maintain business continuity and disaster recovery plans.

Business continuity planning is often thought about in terms technology disaster recovery. However it should be a business-owned and driven process that unifies a broad spectrum of management disciplines. Too many organizations tend to focus all their efforts on their information technology because of its mission-critical nature, leaving them exposed on many other fronts.

BUSINESS CASE:

Recent audits by the Missouri State Auditor have revealed troublesome shortfalls in business continuity and disaster recovery planning in several state agencies. Significantly, the State Auditor has, as the result of audits conducted to date, recognized no state department or agency as meeting minimum standards.

It is estimated that only 25 percent of all organizations have a comprehensive business continuity plan in place today. Ignoring business continuity issues can happen for a number of reasons:

- denial
- lack of understanding
- funding, staffing and time resource constraints
- difficulty in obtaining top management commitment
- difficulty in finding a project leader with the necessary skills

An awareness and training program can help organizations overcome these barriers. This would result in a higher percentage of prepared organizations, thereby improving the State's overall ability to respond to any potential disaster.

ISSUE 2: STATEWIDE METHODOLOGY FOR BUSINESS CONTINUITY PLANNING

- **Awareness and Training**

BENEFITS:

A business continuity plan prepares an organization to ensure the timely and orderly resumption of its critical operations and services in the event of a local or regional disaster. State, Local and nongovernmental organizations would all benefit from an awareness and training program by gaining the knowledge, skills, processes and support required to develop, implement, maintain and execute a comprehensive business continuity plan. Members of the general public would also benefit by having continued access to a greater number critical government and nongovernmental services following a disaster.

COST FACTORS:

The costs of an efficient and effective awareness and training program for Business Continuity would be the additional resources required to analyze the need and implement the appropriate program.

ISSUE 2: STATEWIDE METHODOLOGY FOR BUSINESS CONTINUITY PLANNING

- **Risk Assessment**

In order to maintain and restore critical government services during or after an emergency event, Missouri State governmental agencies must identify and rank the risks associated with potential emergency events which might render Missouri State Government and its agencies inoperable or inaccessible should such an event occur.

BUSINESS CASE:

The delivery of critical state government services is vital to the overall economic vitality of the State of Missouri and its citizens. Failure to realistically assess and address the risks including but not limited to risks associated with a biological incident, civil unrest, earthquake, fire, hazard materials spill, severe heat wave, nuclear attack, nuclear power plant incident, power outages, terrorism, tornado, or severe winter storm, would have significant adverse economic impact on the businesses and citizens of the State of Missouri.

A systematic risk assessment should be conducted for all state agencies of Missouri State Government. It shall be conducted for each state facility and the related function which operates from the facility. The risk assessment should cover the following major issues.

A. Review and documentation of existing disaster recovery and emergency response plans which are currently in place by facility.

B. A definition of the risk assumptions to be utilized in the risk assessment.

C. A definition of the risk factors to be considered.

D. Model for a statewide risk assessment rating.

E. The documentation of the risk assessment results and conclusions.

F. Risk assessment forms which can be used by the state agencies to conduct the respective agencies risk assessment.

And be based on the following priorities:

1. Protect Human Life – Plans should provide a ready means of support and assistance for all injured persons. Other personnel which must remain in a threatened area must be as well protected as possible. Anyone not directly involved in the disaster response should be evacuated to safety.

2. Minimize Personal Injury- State employees should be educated on the nature of the threat and how to respond in order to avoid anyone increasing their personal risk as a result of ignorance or ineptitude.

3. Reduce exposure of Physical Assets – State agencies should avoid storing valuable materials, information or equipment in areas deemed to be vulnerable to an attack.

4. Resumption of Normal Operations – In order to remain operational, state agencies should designate a “pre-determined relocation site” This facility may be used as an

ISSUE 2: STATEWIDE METHODOLOGY FOR BUSINESS CONTINUITY PLANNING

- **Risk Assessment**

emergency headquarters and as a place to temporarily store crucial documents and equipment

5. Designation of Emergency Coordinator – An emergency coordinator should be named for each state facility. The emergency coordinator should have the support of the Director of the state agency and should be able to deal with all levels of the organization.

6. Management Succession Plan – A management succession list with alternative personnel should be developed for each state agency.

BENEFITS:

The benefits of a systematic risk assessment of the agencies and facilities of state government would be the foundation for appropriate and effective business continuity plans. The benefit can be measured in the length of time it would take state government to restore critical services after an event occurs.

COST FACTORS:

The costs of a systematic risk assessment would be the additional resources required to analyze the potential risks along with the cost of implementing appropriate preventative and recovery strategies.

ISSUE 2: STATEWIDE METHODOLOGY FOR BUSINESS CONTINUITY PLANNING

♦ Business Impact Assessment

In order to respond to disruptive events, Missouri state agencies must develop contingency plans tied to their critical responsibilities and the underlying infrastructure. Starting with a prioritized inventory of agency business functions/processes, the agency can identify critical business applications and the supporting infrastructure. The resulting Business Impact Analysis (BIA) will be used to develop Business Continuity Plans, quantify risks and secure funding to mitigate potential outages.

An agency BIA should:

- Identify critical business functions, the impact of disruption, and the business requirements for the maximum allowable outage period.

- Identify the underlying applications and IT resources such as Internet connectivity, building connectivity, application servers, mass storage, workstations, etc on which these critical business functions depend.

- Identify the staffing dependencies for these systems.

- Identify utility and building infrastructure dependencies such as HVAC, electricity, etc.

- Determine the inter-relationships between IT resources, applications and staffing to determine recovery bottlenecks and critical path activities.

- Identify single points of failure and high probability combinations of events that will cause an disruption.

- Identify mitigation strategies and any required funding.

BUSINESS CASE:

In order to meet mission requirements and public expectations, state agencies need to prioritize both their business functions and their response to business disruptions. Agencies should be able to quantify the impact of disruptions to business functions in terms of financial costs and loss of the public trust.

These priorities and costs should be used to guide decisions on mitigation strategies and order of recovery activities.

ISSUE 2: STATEWIDE METHODOLOGY FOR BUSINESS CONTINUITY PLANNING

- **Business Impact Assessment**

BENEFITS:

The BIA should be the vehicle by which agency business units and supporting IT units analyze dependencies between business functions and underlying infrastructure as well as establish shared priorities for mitigating outages and recovering from disruptions.

Agency management should be able to use the BIA analysis to secure funding for specific risk mitigation activities or share the unmitigated risk with agency stakeholders.

COST FACTORS:

Cost of ***developing*** a BIA is highly dependent on the number of business processes to analyze and the complexity and interdependence of the underlying systems. BIA development costs can be mitigated by re-tasking staff, pre-existing formal business function risk assessments, agency Memoranda of Understanding (MOU), Service Level Agreements (SLA), or cost/benefit analyses.

Costs of ***implementing*** mitigation strategies can range from very inexpensive for process changes and migration of applications to an alternate system resource to very expensive for replacing or duplicating existing systems.

ISSUE 2: STATEWIDE METHODOLOGY FOR BUSINESS CONTINUITY PLANNING

♦ **Business Continuity Strategies**

Missouri State Government must determine and guide the selection of alternative business recovery operating strategies for recovery of business and information technologies within the recovery time objective, while maintaining the organization's critical functions.

BUSINESS CASE:

Recovery strategies should provide a means to restore operations timely and cost effectively following a service disruption. Business strategies as well as Information Technology strategies must both be addressed. Strategies should be developed in the light of cost/risk/benefit analysis addressing the disruption impacts and allowable outage times identified in the BIA.

Several alternatives should be considered when developing the strategies, including cost, allowable outage time, security, and customer impact. Business strategies should consider not only traditional alternatives but also unique alternatives such as an interim alternative organizational hierarchy to provide quicker issue identification, decision and resolution. Alternative short-term operational processes are also worthy of consideration.

The selected recovery strategy should address the potential impacts identified in the BIA and should be integrated into the system architecture during the design and implementation phases of the system life cycle.

Business recovery strategies should address such issues as -

- Physical Facilities
- Workgroup Recovery
- Work Area Recovery
- Technology Infrastructure
- Data and Voice Communications
- Data
- Customer Service (Help Desk)
- Training
- Security

ISSUE 2: STATEWIDE METHODOLOGY FOR BUSINESS CONTINUITY PLANNING

♦ Business Continuity Strategies

A wide variety of recovery approaches may be considered; the appropriate choice depends on the incident, type of business, and its operational requirements. Specific recovery methods may include:

- Alternate Sites
  a. Hot - High Availability
  b. Warm - Short time delay
  c. Cold - Start Up Sites
- Contracts
- Reciprocal Internal or External Agreements
- Service Level Agreements
- Alternative technological environment
- Combination of Alternatives

The strategy may include a combination of methods that complement one another to provide recovery capabilities over the full spectrum of incidents.

Obtaining written contractual agreements with specified terms and conditions when utilizing external resources and vendors for specific recovery alternatives should be embedded into any fundamental strategy.

BENEFITS:

The right combination of business and technology strategies allow the development of efficient and effective plans to support executive and management priorities providing timely, cost effective, recovery of business and technological operations

COST FACTORS:

Actual cost is dependent upon a wide variety of variables. However, utilizing the Business Impact Analysis, as a guideline and performing cost/risk/benefit analysis for each process should yield timely, cost effective, solutions.

ISSUE 2: STATEWIDE METHODOLOGY FOR BUSINESS CONTINUITY PLANNING

♦ **Business Continuity Plans**

Missouri State Government must design, develop, and implement Business Continuity Plans that provide timely recovery and restoration of essential services to the public. Business Continuity Plans are a fundamental enabler of disaster response, consequence management efforts by Government. In the absence of detailed, realistic plans, Continuity of Government is placed at risk. Business continuity plans have historically not been developed in support of any unified strategy. Plans must be owned and maintained by each state entity. Plan development is one of the most important parts of Business Continuity Management. Failure to have realistic, achievable Business Continuity Plans fails to satisfy the fundamental obligations of state government.

BUSINESS CASE:

State Government routinely experiences loss of capability resulting from natural disaster, man-made event, and equipment failure. Terrorism, weapons of mass destruction and the global war on terror introduce new and significant threats to State Government. Currently, most State agencies/activities lack achievable Business Continuity plans that ensure their ability to provide timely service to the public.

Ironically, it is during times of disaster and consequence management that the public's demand for government services is greatest. It is essential that all elements of state government develop, test and implement business continuity plans.

The Missouri Security Panel report (February 2002) recommended assessment of all critical infrastructure, including information systems. The *National Strategy for The Physical Protection of Critical Infrastructures and Key Assets* (February 2003); states "America's critical infrastructure sectors provide the foundation for our national security, governance, economic vitality, and way of life. Furthermore, their continued reliability, robustness, and resiliency create a sense of confidence and form an important part of our national identity and purpose." The National Governors Association publication, *A Governor's Guide to Emergency Management, Volume Two: Homeland Security* (September 2002); "addresses the major homeland security issues a governor and his or her staff need to understand and prepare for,…and outlines the interaction needed among the governor's office, the homeland security director, the state emergency management office, other state agencies, local governments, the private sector, volunteer organizations, and the federal government."

Business Continuity Plans are designed to address the needs of the organization on different levels. At the highest level there is a need for a Crisis Management process and plan. Continuity plans must address damage assessment, salvage, public relations, and protection of vital records.

Continuity Plans must be "scenario based" and address service disruption, ensure the safety of personnel and to implement the business recovery process. There are key support functions that must be addressed (Accommodation and Services, Computer Systems and Network, Telecommunications, Security, Personnel and Finance and Administration)

Frequently, agencies will start Business Continuity planning the Information Technology functional area. This focused effort will address recovery of computer systems, network and telecommunications in a disaster situation once a decision to invoke the process has been made. The plan must contain details of how lost data can be recovered and reconciled and how systems

ISSUE 2: STATEWIDE METHODOLOGY FOR BUSINESS CONTINUITY PLANNING

- **Business Continuity Plans**

recovered to different points can be aligned. The plan should manage return to normal operations once the incident has been resolved. Procedural documentation supporting the IT recovery plan should include systems and application restoration procedures, 'run-books' detailing the order of recovery of applications and data, business driven data reconciliation, data integrity checking, and security permissions.

Each critical business area is responsible to develop a plan defining individuals who are in recovery teams, and a detailed task list for the recovery process. The owners of each plan must address outside parties upon whom they rely for a service or resource. Plans must be easily accessible, and distributed to all personnel who have a part to play in a recovery.

BENEFITS:

Providing essential public services in a disaster response/consequence management effort is assured by development, testing and implementation of Business Continuity Plans. Risks are reduced, quality of support is improved, and the confidence of the public is maintained,

COST FACTORS:

Generally, cost associated with plan development will be absorbed by activities within existing resources. It is anticipated that the incremental costs associated with plan development will be offset by cost avoidances generated by reduced loss of productivity.

ISSUE 2: STATEWIDE METHODOLOGY FOR BUSINESS CONTINUITY PLANNING

♦ **Testing and Exercising Business Continuity Plans**

Testing and exercising Business Continuity plans support and validate Emergency Management Plans. Missouri state government and its subordinate agencies must routinely test the validity of Business Continuity Plans. The operating environment (facilities, information technology, personnel) is dynamic. Routine testing maintains the accuracy achievability and relevance of plans.

BUSINESS CASE:

Emergency Management Plans deal with the "operational" delivery of Governmental services to the public. Business Continuity plans ensure that the agency/activity maintains the ability to support internal capabilities (communications, personnel, facilities, etc.) essential to generating public services. Routine, predictable testing and exercising plans creates the opportunity for staff assessment and validation of the linkage between the two efforts.

Business Continuity plans are most relevant if the are "scenario based" and have defined facts and assumptions concerning the threat, the environment and the anticipated response requirements. Constant change in infrastructure, personnel, and resources undermine the accuracy and reliability of the Plan. Routine and realistic testing is essential to train staff, validate processes, develop understanding and reduces probabilities of failure.

Missouri State Government must pre-plan and coordinate plan exercises, and evaluate and document exercise results. An objective of testing is to develop processes to maintain the continuity capabilities and document plans in accordance with the organization's strategic direction. Testing will also verify that the Plan will prove effective by comparison with a suitable standard, and report results in a clear and concise manner. Business continuity plans and associated testing ensure that maintenance is undertaken on a regular basis.

A program for maintaining and exercising plans must be established to ensure that the critical components remain current. It is important that any changes to the IT infrastructure are addressed in the plan, implemented in an appropriate fashion and evaluated to ensure that they function correctly within the overall provision of services. Testing the plan is a requirement to maintain the awareness of responsibilities and also to ensure train new employees. Testing will raise the level of confidence in the ability to recover from a systems failure. It will provide staff members with a standard awareness and training processes within the organization.

Technical tests must involve the business as a whole. This will help to prove capability, and aid mutual understanding of the activities and resources needed to achieve the common goal of business recovery. The test must validate completeness of the plans and confirm:

- Time objectives. For example, time taken to recover key server applications
- Staff preparation and awareness.
- Staff duplication and potential over commitment of key resources. For example, a system administrator being required to support a number of modular plans (help desk, operations, networks and communications).
- Responsiveness, effectiveness and awareness of third parties and service providers.

ISSUE 2: STATEWIDE METHODOLOGY FOR BUSINESS CONTINUITY PLANNING

- **Testing and Exercising Business Continuity Plans**

It is also necessary to ensure that the business recovery personnel are tested. This can include familiarization with the recovery site, and the provision of walkthrough tests that will exercise the team response to a relevant scenario. All tests, whether technical or non technical must have clearly defined objectives and critical success factors which will be used to determine the success or otherwise of each exercise. Obtaining assurance in the quality of the plan must be undertaken as part of the internal and external audit process and can be used to demonstrate the efficiencies and effectiveness of the Business Continuity environment.

BENEFITS:

Routine testing ensures that State Agencies are capable of providing critical services to the public. Testing is ensures that the vitality and accuracy of the plan is maintained. Most importantly, testing ensures that the Business Continuity Plan supports the strategic goals of Emergency Management plans..

COST FACTORS:

The greatest incremental cost of testing is the investment of time by existing staff members. Given that testing trains critical personnel to be better prepared to provide essential services in a disaster, this could easily be considered high payoff education/professional development costs. Additional funding (outside of existing agency-specific resources) specifically to support training is not required.

ISSUE 3: COORDINATION EFFORTS

- **Emergency Management Plans**
- **Public Relations Management**
- **Coordination with Public Authorities**

ISSUE DESCRIPTION:

Many organizations believe crises only happen to others and that there size or some other feature makes them immune. They genuinely believe 'It will not happen to us'. Although bombs, fires and floods capture the headlines almost 90% of crises are 'quiet catastrophes'. It is these quiet catastrophes that also have the potential to damage your organization's most valuable assets; its reputation. These can be destroyed very quickly unless vigorously defended at times when the speed and scale of events can overwhelm the normal operational and management systems.

In managing any event it is critical to recognize that a successful outcome is judged by both the technical response and the perceived competence and capability of the management delivering the response. The stakeholder perception should be seen as the critical success factor with an equal if not more urgent priority over the technical solution. Consequently, the 'acid test' is to convincingly demonstrate an efficient and effective Business Continuity Management competence and capability for continuing business.

AUTHORIZATION:

Code of State Regulations: Title 11 - Department of Public Safety, Division 10 – Adjutant General, Chapter 11 – State Emergency Management Agency. 11 CSR 10-11.010 Emergency Operations Plan (State). PURPOSE: The State Emergency Management Agency, Office of the Adjutant General has the authority to establish a plan to organize the state government in order to respond in an emergency and to provide guidance to state agencies and local political subdivisions in the preparation of disaster plans of their own as required by sections 44.010 and 44.090, RSMo.

ACTION REQUIRED:

The State Emergency Management Agency (SEMA), Department of Public Safety is responsible to maintain copies of Business Continuity plans for all State agencies. SEMA will report annually, those agencies that have failed to provide and maintain Business Continuity Plans.

The Director of Public Safety, supported by the Office of Information Technology will coordinate Disaster Response/Business Continuity technology resources required to support communications and Information Technology. The objective is to ensure that critical capabilities are provided without interruption, and restoration of other services is planned in sufficient detail to ensure success.

ISSUE 3: COORDINATION EFFORTS

♦ Emergency Management Plans

Missouri State governmental agencies must have emergency management plans in place for responding to and stabilizing a situation following an emergency incident or event. While the State has an overall Emergency Management Plan (EMP) for responding to regional disasters most State agencies do not have a comprehensive agency EMP for dealing with more localized emergencies. Emergency Management Plans focus on the measures that are essential for protecting live and property.

An agency EMP is a document that:

- Assigns responsibility to organizations and individuals for carrying out specific actions at projected times and places in an emergency.
- Sets forth lines of authority and organizational relationships, and shows how all actions will be coordinated.
- Describes how people and property will be protected in emergencies.
- Identifies personnel, equipment, facilities, supplies, and other resources available--within the agency or by agreement with other agencies--for use during response and recovery operations.
- Identifies steps to address mitigation concerns during response and recovery activities.

BUSINESS CASE:

Every year emergencies take their toll in lives and dollars. When an emergency threatens or strikes, people expect the State to take immediate action to deal with the problem. An EMP would provide procedures in the event of a situation posing a potential threat to the health and safety, the environment, and/or property. Such events include but are not limited to a biological incident, civil unrest, earthquake, fire, hazard materials spill, severe heat wave, nuclear attack, nuclear power plant incident, power outages, terrorism, tornado, or severe winter storm. While most State agencies have fire and tornado evacuation plans/procedures many are not prepared to address a number of other potential hazardous situations.

BENEFITS:

An EMP would help State agencies be prepared to fulfill their responsibility to protect lives and property of all Missourians when an emergency incident or event threatens the health and safety, environment, and/or property.

COST FACTORS:

The cost of developing an EMP by each agency cannot be estimated with any accuracy, but should be minimal.

ISSUE 3: COORDINATION EFFORTS

- **Public Relations Management**

Missouri State Government must develop, coordinate, evaluate, and exercise plans to handle media during crisis situations and to communicate with and, as appropriate, provide trauma counseling for employees and their families, key customers, critical suppliers, owners/stockholders, and corporate management during crisis. This must be done to ensure all stakeholders are kept informed on an as-needed basis.

BUSINESS CASE:

Crises or disasters can strike at any time. They are most devastating when sudden, but slower events can be cumulative and just as damaging. When crises or disasters happen, there needs to be a practiced plan that ensures a positive, focused and effective response. During such events there tends to be confusion, uncertainty and even fear. A crisis management plan generates order out of chaos. It needs strong leadership by well trained and rehearsed individuals. Everyone within an organization should know what their role is in a crisis, and what they have to do.

It is often thought that a business with a good crisis management plan does not need Business Continuity Plans. This is wrong. There are two key phases undertaken when responding to a crisis:

- Response
- Recovery

Crisis management deals with the immediate response to a crisis, but also ensures that business continuity plans can be invoked, executed effectively and managed. Business continuity plans deal more with the recovery phase. The subject, when including both crisis management and business continuity, is often referred to as Integrated Emergency Management. The two subjects are interrelated but separate subjects, both of which have at their heart an assessment of risk. This issue deals with crisis management.

A crisis can be defined as an abnormal situation, or even perception, which is beyond the scope of everyday business and which threatens the operations, safety and reputation of an organization. Crisis management is the process by which the organization manages a wider impact, such as media management, and enables the business to commence recovery. By definition, crisis management deals with incidents of major impact. The subject is separate from (but integrated with) business continuity. A good crisis management plan without sound continuity planning is like building a house on clay. There is also a dichotomy in crisis management planning. The best plans are the simplest and yet the attention to detail remains extremely important. The role of the Crisis Management Team (CMT) within a business is a straightforward management process. It should:

- Establish what has happened
- Assess the impact
- Resolve any conflicts of interest
- Identify and prioritize actions required
- Retain Control

ISSUE 3: COORDINATION EFFORTS

♦ **Public Relations Management**

BENEFITS:

The benefits of effective crisis management are numerous and immediate. They include:

- Enhanced safety for staff and customers
- Compliance with regulatory and ethical requirements
- Effective management of major incidents
- Increased staff awareness of the organization
- Increased confidence and morale within the organization
- Protected and often enhanced reputation
- Reduced risk of litigation
- Levels of control and authority limits

COST FACTORS:

There is no guarantee that a business will survive a major disruption to its service, even if it is caused by an incident outside its control. It is interesting to note that some companies now fund crisis management from their sales and marketing budget, rationalizing that good crisis management ensures a robust and resilient service; something customers demand. The crisis management team would normally prepare a brief for the organization. This is often done with the help of a Public Information Officer (or equivalent), as the brief also forms the basis of a common message, communicated to appropriate external organizations (including the media).

ISSUE 3: COORDINATION EFFORTS

♦ Coordination with Public Authorities

Missouri State Government must establish applicable procedures and policies for coordinating response, continuity, and restoration activities with local, state, and federal authorities while ensuring compliance with applicable statutes or regulations. The crisis management process identifies those functions that are essential in carrying out business continuity operations in the event of a disaster situation. Through the development of business continuity plans, state government will ensure that a process is in place that keeps all stakeholders informed on an as-needed basis.

BUSINESS CASE:

State government is responsible for providing services to its citizens and business partners on a daily basis. The possibility exists for man-made or natural disasters that can disrupt these services for short or long periods of time. The possibility also exists for limited access to specific buildings or areas that could disrupt service for undetermined time periods.

To minimize the impact to the citizens, the government must initiate a Business Continuity Plan that includes coordination at the levels most affected by the disruption. Currently, not every state agency or entity has a business continuity plan to continue operations a various levels due to disruption of services. A key area that must be addressed in any business continuity plan is the process of coordination between the entities charged with responding to the event and assisting with recovery operations.

Missouri State Government is also responsible for the development and maintenance of the State Emergency Operations Plan (SEOP). The SEOP lays a framework that will allow the State of Missouri to save lives, minimize injuries, protect property and the environment, preserve functioning civil government, insure constituted authority, and maintain economic activities essential to the response and recovery from natural, technological and national security hazards.

The SEOP outlines actions to be taken by state government and other participating organizations which will 1) prevent avoidable disasters; 2) reduce the vulnerability of jurisdictions to their effects; 3) establish response capabilities; 4) maximize the effectiveness of state response and 5) speed recovery. The SEOP also sets the parameters for the development of local emergency operations plans and procedures.

BENEFITS:

The public expects government to function not only before an emergency but also during, and after an emergency. The public is unwilling to overlook interruptions in services, even in the event of disasters – especially service involving public safety and health. The public expects good “customer service” of the government as much as it does from business. By having business continuity plans in place, government will continue to function and ensure that lives are saved, property is protected, and service will continue.

ISSUE 3: COORDINATION EFFORTS

♦ Coordination with Public Authorities

By establishing the key links between state government and local and federal authorities throughout the state, the government can continue to provide the following benefits:

- State, Local, and Federal authorities are equally informed.
- Local authorities can provide service and guidance based on current information.
- Information flow is continuous at all levels to ensure compliance.

COST FACTORS:

The cost associated with establishing policies and procedures for coordination with public authorities should be minimal considering law enforcement, SEMA, MONG, and other government entities have communication systems in place to notify local and related authorities concerning situation status and proper procedures.

However, costs can vary widely depending on the complexity and sophistication of the coordination methods and techniques. If a more advanced system is desired for security and notification, costs can escalate for a separate system.